North Arlington Public Schools

High School, Middle School, Jefferson, Roosevelt, Washington
201-991-6800

SCHOOL TECHNOLOGY DEVICE LENDING AGREEMENT

School district-provided technology devices may be signed-out for specified timeframes and under certain circumstances, which will require pre-approval by District Administration. Upon approval, both the parent/guardian and student will agree and adhere to the following:

- *Device will only be used by the student for educational purposes as directed and/or required*
- *Compliance with our Acceptable Use Polices and other technology policies in effect at the time*
- *Any damage, theft, or loss of device will be reimbursed to the school by parent/guardian*
- *Student is required to report any damage or malfunctions during the period of time the device is assigned to them*
- *If stolen, parent/guardian/student are required to file a police report and notify school personnel*
- *Student will use the device at home and/or bring the device to school as directed or required*
- *All other provisions described further in District Policies: 2361, 7523, and District Regulation 2361.*

Date Signed Out:	
Purpose/Reason:	
Parent/Guardian Name:	
Parent/Guardian Primary Phone #:	
Parent/Guardian Signature:	
Student Name:	
Student Signature:	

This section to be completed when the technology is returned to the school

Date Returned:	
Any Visual Defects:	
School's Signature:	

NOTICE: This device might be equipped with a camera, GPS, or other recording or collection feature, and we may record or collect information on the student's activity and the student's use of the device. The district shall not use any of these features in a manner that would violate the privacy rights of the student or any individual residing with the student.

This document is to be kept on file by the school where the technology was borrowed. A copy of this document is to be sent to the Office of Technology upon signing, and another copy must be sent when the technology is returned.

logo

North Arlington Board of Education

Home

< Prev | Next >

To Regulation

Search District Policies

District Policies TOC

District Policy

2361- ACCEPTABLE USE OF COMPUTER NETWORK/COMPUTERS AND RESOURCES (M)

Section: Program
Date Created: October 2008
Date Edited: June 2013

M

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 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 with the Principal's Office 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: 3 June 2013

logo

North Arlington Board of Education

Home

< Prev | Next >

To Regulation

Search District Policies

District Policies TOC

District Policy

7523- SCHOOL DISTRICT PROVIDED TECHNOLOGY DEVICES TO STUDENTS

Section: Property
Date Created: May, 2017
Date Edited: May, 2017

The Board of Education may provide technology devices to students in the district for school district authorized use only. The purpose of this Policy is to establish general guidelines for the issuance and utilization of any school district technology device provided to students of this district. For the purposes of this Policy, "technology device" or "device" shall include, but not be limited to, portable devices such as computers, laptops, tablets; cellular telephones, or any other computing or electronic devices the school district provides to students to be used as part of their educational program.

A technology device made available to students will not be considered a textbook or supply, as defined in N.J.S.A. 18A:34-1, mandatory to a successful completion of the classroom curriculum. Therefore, because a technology device defined in this Policy is not mandatory to a successful completion of a student's classroom curriculum, a student will not be required to obtain a technology device provided by the school district as defined in this Policy. In the event the school district provides a technology device that is deemed mandatory to a successful completion of the classroom curriculum, the district will provide students with such a technology device consistent with its textbook or supply policies. Nothing in this Policy prohibits a student from using their personal technology device in accordance with school rules and regulations.

A technology device provided by the school district may include pre-loaded software. A student is prevented from downloading additional software onto the technology device or tampering with software installed on the technology device. Only school district authorized staff members may load or download software onto a school district provided technology device.

To receive a school district provided technology device, the parent and student must sign a School District Provided Technology Device Form requiring the parent and the student to comply with certain provisions. These provisions may include, but are not limited to:

1. A school district provided technology device must be used only by the student for school district authorized use;

2. A student shall comply with the school district's acceptable use of technology policies, which shall be attached to the School District Provided Technology Device Form, in their use of any school district provided technology device;

3. Any school district provided technology device loaned to a student must be returned to the school district in the condition it was initially provided to the student considering reasonable use and care by the student;

4. The parent or student shall be responsible to reimburse the school district the cost of any technology device that is lost, damaged beyond reasonable use or beyond its value, abandoned, missing, stolen, or cannot be returned to the district in accordance with the terms of the School District Provided Technology Device Form;

5. The district may require, or offer as an option, depending on the type of technology device provided to the student, an insurance policy to be purchased by the parent or student that would cover certain losses or damage to a technology device during the time period the student has possession of the device. The parent or the student shall pay any insurance policy required deductibles in the event of a loss;

6. In the event the school district does not require the purchase of an insurance policy for a technology device or the parent or student elects not to purchase optional insurance, the parent and/or student shall be responsible for any loss or damage to the technology device in accordance with the terms of the School District Provided Technology Device Form;

7. A student will be required to report any hardware or software problems in the operation of the device to the school district staff member, designated on the School District Provided Technology Device Form, within two school days of the commencement of the problem;

8. A student must report to the school district staff member designated on the School District Provided Technology Device Form within two school days in the event the technology device has been damaged or is missing;

9. A parent or student is required to immediately file a police report in the event it is believed the technology device has been stolen. Within one school day after filing a police report, a parent or student shall complete the School District Provided Technology Device Loss Form and submit the completed Loss Form and a copy of the police report to the Principal or designee;

10. A student shall be required to provide routine cleaning and care of the device in accordance with school district cleaning and care guidelines;

11. The student shall have the technology device in their possession in school as required; and

12. Any other provisions the Superintendent of Schools determines should be included on the School District Provided Technology Device Form.

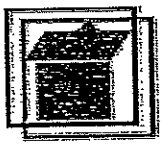
The school district will provide the student and parent with written or electronic notification that the technology device provided by the school district may record or collect information on the student's activity or the student's use of the technology

device if the 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. This notification shall also include a statement that the school district 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 shall be required to acknowledge receipt of this notification and the parent acknowledgement shall be retained by the Principal or designee for as long as the student retains the use of the school district provided technology device. The parent acknowledgement and a signed School District Provided Technology Device Form shall be required before the issuance of a technology device to a student. In accordance with the provisions of P.L. 2013, Chapter 44, a school district failing to provide this notification shall be subject to a fine of $250 per student, per incident. The fine shall be remitted to the New Jersey Department of Education, and shall be deposited in a fund that shall be used to provide laptop or other portable computer equipment to at-risk students as defined in N.J.S.A. 18A:7F-45.

Students shall comply with all school district policies for the use of a school district provided technology device. A student shall be subject to consequences in the event the student violates any school district policy, including the district's acceptable use policies; student code of conduct; any provision of this Policy; or any provision of the School District Provided Technology Device Form.

N.J.S.A. 18A:34-1
P.L. 2013, Chapter 44 – "The Anti-Big Brother Act"

Adopted: May 22, 2017



logo

North Arlington Board of Education

Home

< Prev | Next >

To Policy

Search District Regulations

District Regulations TOC

District Regulation

2361 - ACCEPTABLE USE OF COMPUTER NETWORK/ COMPUTERS AND RESOURCES

Section: Program
Date Created: October 2008
Date Edited: June 2013

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.

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.

Adopted: 03 June 2013