



Clinton Township Middle School
34 Grayrock Road, Clinton, NJ 08809
Community & Teamwork Motivate Success

Judith B. Hammond, Principal
Phone: 908-238-9141
Fax: 908-238-9376
Jhammond@ctsdnj.org

Michele Cone, Asst. Principal
Phone: 908-238-9141
Fax: 908-238-9376
MCone@ctsdnj.org

Dear CTMS Parents/Guardians:

Enclosed are the School Furnished Device Usage Agreement, School Furnished Electronic Device Student Responsibility Contract, and accompanying Board of Education policies and regulations (6142.10, 3514.1) which will govern the CTMS 1:1 program. The students will begin receiving their assigned chromebooks on Monday, November 28. In order to receive a chromebook on November 28, please complete the following steps:

1. Review the attached Device Usage Agreement and BOE policies with your student(s).
2. Review and sign the School Furnished Electronic Device Student Responsibility Contract (parent(s) and student(s)).
3. Return the signed School Furnished Electronic Device Student Responsibility Contract to Clinton Township Middle School on Monday, November 28, 2016.
4. Students will submit the contract and be issued their assigned chromebook during the morning of Monday, November 28, 2016.

We are looking forward to the launch of our 1:1 program. If you have any questions, please feel free to contact us.

Sincerely,

Ms. Judith Hammond, Principal, CTMS
Mrs. Michele Cone, Assistant Principal, CTMS
Mr. Timothy Jaw, Supervisor of Technology, CTSD



Clinton Township Middle School
34 Grayrock Road, Clinton, NJ 08809
Community & Teamwork Motivate Success

Judith B. Hammond, Principal
Phone: 908-238-9141
Fax: 908-238-9376
JHammond@ctsdnj.org

Michele Cone, Asst. Principal
Phone: 908-238-9141
Fax: 908-238-9376
MCone@ctsdnj.org

School Furnished Electronic Device Usage Agreement

Students shall adhere to the following guidelines when using school furnished electronic devices:

1. Use of the electronic device is subject to the Clinton Township School District's ("District") policies and regulations, including Policy 6142.10, (Internet Safety and Technology), Policy/Regulation 3514.1 (School Furnished Electronic Device: Distribution and Use), and Policy/Regulation 5131 (Code of Student Conduct). The District's policies and regulations can be found on the District's website: http://ctsdnj.org/board_of_education/policy
2. The Student shall be provided with certain privileges and rights on the district's network. The Student should in no way attempt to gain other privileges or to attempt to access resources on the network to which no explicit rights have been granted.
3. The Student shall not, in any way, tamper with or misuse school equipment, either software or hardware. No form of tampering is acceptable.
4. The Student may not download copyrighted software, audio or video files, or any other copyrighted material from the Internet not legally allowed to be used. Any such material found will be deleted without prior notification.
5. The electronic device may include the district's software image and preloaded software for specific tasks. The installation of other software images or software shall be approved and may only be done by the assigned staff member authorized to maintain the equipment.
6. Software in use in the District is licensed in a correct and legal manner. The Student should make no attempt to copy licensed or copyrighted material using this electronic device.
7. The electronic device shall be used for the sole and express purpose of conducting school work and may not be used for any form of personal financial gain.
8. This electronic device and its contents remain the property of the District. It shall be returned by the Student at the end of the school semester or school year as assigned. No data stored on this electronic device is personal or private and the Student has no reasonable expectation of privacy in such data. Any application or data (apps, music, etc...) will become the property of the District upon completion of the program.

9. The Student issued the electronic device shall have no expectation of privacy in the use of such device. The electronic device may have security settings, monitoring or auditing software, tracking technology, and any other software that could monitor the use of the technology device.
10. This 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. If school district equipment is issued to a student for use outside the district, it is possible this collection of information on the student's activity or use of the device may occur outside of the school. 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 as per *N.J.S.A. 18A:3639*.
11. The Student is expected to take all appropriate measures and precautions to prevent the loss, theft, damage, and/or unauthorized use the electronic device. Appropriate measures and precautions taken by the Student shall include, but are not limited to:
 - a. Keep the electronic device in a locked and secured environment when not being used;
 - b. Do not leave the electronic device in a vehicle for prolonged periods of time, especially in extreme temperatures;
 - c. Keep food, drinks, and liquids away from the electronic devices and work areas;
 - d. Do not lend the electronic devices to any other person unless authorized to do so by the Superintendent or his or her designee;
 - e. Store the electronic device when not in use only in a securely locked area;
 - f. Do not leave the electronic device unattended at any time in an unsecured location; and
 - g. Keep the school furnished electronic device in sight at all times while in public places.

Resulting damage to the electronic device may not be covered by warranties, and the Student may be liable for repair costs. The parent/guardian shall be responsible to reimburse the school district the cost of any electronic device that is lost, damaged beyond reasonable use or beyond its value, abandoned, missing, stolen, or cannot be returned to the District. The Board of Education is under no legal, financial, or other obligation to provide a replacement electronic device to any Student whose device is lost, stolen, or damaged.

12. The Student is required to provide routine cleaning and care of the electronic device as needed.

13. When the Student has reason to believe the electronic device may have been stolen, they must:
 - a. Immediately report the incident to the issuer of the device;
 - b. File an official police report documenting the theft; and
 - c. Provide a copy of the police report to the school.
14. The Student must report any hardware or software problems in the operation of the device to assigned staff members authorized to maintain the equipment.
15. The Student is responsible for having the electronic device fully charged for class or classes in which the device will be used. Failure to have the device in class or not charged for class may result in disciplinary action for being unprepared for class.

Use of electronic device resources are granted based on the Student's acceptance of the following responsibilities:

1. Use only those computing and information technology resources for which authorization is given. For example, it is a violation to:
 - a. use resources that you have not been specifically authorized to use;
 - b. use someone else's account or password or share your account or password with someone else;
 - c. access files, data or processes without authorization; or
 - d. purposely look for or exploit security flaws to gain system or data access.
2. Use computing and information technology resources only for their intended purpose. For example, it is a violation to:
 - a. send forged email;
 - b. misuse Chat or other communications software that appears to allow students to hide their identity or to interfere with other systems or students;
 - c. use electronic resources for harassment, intimidation, bullying or stalking other individuals;
 - d. send bomb threats or "hoax messages";
 - e. send chain letters;
 - f. intercept or monitor any network communications not intended for you;
 - g. use the network to facilitate illegal activity;
 - h. use the network for commercial or for profit purposes;
 - i. use the network for non-school related work on more than an incidental basis;
 - j. use the network for product advertisement or political lobbying;
 - k. use the network for hate mail, discriminatory remarks, and offensive or inflammatory communication;

- l. illegally install, distribute, reproduce, or misuse copyrighted materials;
 - m. use the network to access obscene or pornographic material;
 - n. use inappropriate language or profanity on the network.
 - o. use the network to transmit material likely to be offensive or objectionable to recipients;
 - p. use the network to intentionally obtain or modify files, passwords, and data belonging to other users;
 - q. use network facilities for fraudulent copying, communications, or modification of materials in violation of copyright laws;
 - r. use the network to disrupt the work of other users;
 - s. use computing or network resources for advertising or other commercial purposes to attempt to circumvent security mechanisms;
 - t. load or use unauthorized games, programs, files, or other electronic media;
 - u. destroy, modify, or abuse network hardware and software;
 - v. quote personal communications in a public forum without the original author's prior consent; or
 - w. participate on unauthorized social networks.
3. Protect the access and integrity of computing and information technology resources. For example, it is a violation to:
- a. release any software (i.e. malware) that damages or harms a system or network;
 - b. prevent others from accessing an authorized service;
 - c. send email bombs that may cause problems and disrupt service for other students;
 - d. attempt to deliberately degrade performance or deny service;
 - e. corrupt or misuse information;
 - f. alter or destroy information without authorization; or
 - g. share your district password with, or allow a password to be used by, anyone else.
4. Abide by applicable laws and school policies and respect the copyrights and intellectual property rights of others, including the legal use of copyrighted software. For example, it is a violation to:
- a. make more copies of licensed software/content than the license allows;
 - b. download, use, or distribute pirated software/content;
 - c. operate or participate in pyramid schemes;
 - d. distribute or view pornography on the device; or
 - e. upload, download, distribute, or possess child pornography.
5. Respect the privacy and personal rights of others. For example, it is a violation:

- a. to run network sniffing/monitoring tools without authorization;
- b. Impersonate another user;
- c. to access or attempt to access another individual's password or data without explicit authorization; or
- d. to access or copy another student's electronic mail, data, programs, or other files without permission.



Clinton Township Middle School
34 Grayrock Road, Clinton, NJ 08809
Community & Teamwork Motivate Success

Judith B. Hammond, Principal
Phone: 908 -238-9141
Fax: 908-238-9376
JHammond@ctsdnj.org

Michele Cone, Asst. Principal
Phone: 908-238-9141
Fax: 908-238-9376
MCone@ctsdnj.org

School Furnished Electronic Device Student Responsibility Contract

Student Name: _____

Student Grade: _____

I have read, understand, and agree to adhere to the following attached documents:

1. School Furnished Electronic Device Usage Agreement;
2. Clinton Township Board of Education Policy 6142.10, Internet Safety and Technology, which includes Acceptable Use of Technology; and
3. Clinton Township Board of Education Policy and Regulation 3514.1, School Furnished Electronic Device: Distribution and Use.

I understand that the district technology is for educational purposes only and that the school district has taken reasonable steps to safeguard the access for users. However, I understand that it is not possible to stop all inappropriate activities and I will not hold the district responsible for any materials obtained through the use of the networks and/or electronic device.

The electronic device may record or collect information on my 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 my activity or use of the device. It is possible this collection of information on the student's activity or use of the device may occur outside of the school. 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 as per N.J.S.A.18A:3639.

I understand that if this electronic device is lost or stolen, I will immediately notify the District. I understand that the District shall not be responsible for any damages or losses related to this electronic device. Any costs associated with instances of loss, theft or damage may be the full responsibility of the student and his/her parent/guardian.

I agree to return this electronic device to the District at the conclusion of the school year (or earlier if I should leave the District). I further understand any application or data (apps, music, etc...) loaded on the device become the property of the school district and will not be returned.

I understand that failure to comply with any of these rules, policies or procedures, including, but not limited to, misusing the Internet or electronic device, accessing unauthorized Internet locations, or participating in any activities that violate of Board Policy 6142.10 (Internet Safety and Technology) or Board Policy/Regulation 3514.1 (School Furnished Electronic Device: Distribution and Use), may result in disciplinary action, including the revocation of the Agreement, immediate return of the device to the District, and/or suspension or expulsion in accordance with the school Code of Student Conduct (Board Policy/Regulation 5131). In addition, criminal activity will be referred to the appropriate authorities.

_____	_____	_____
Print Student Name	Student Signature	Date
_____	_____	_____
Print Parent/Guardian Name	Parent/Guardian Signature	Date

Policy

INTERNET SAFETY AND TECHNOLOGY

The Clinton Township Board of Education 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 state-approved mathematics and language arts and literacy.

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).

COMPLIANCE WITH CIPA

Filters Blocking Access to Inappropriate Material

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.

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:

- A. Unauthorized access, including so-called "hacking," and other unlawful activities; and
- B. Unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

Education, 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 Superintendent or his or her designee.

The Superintendent or his or her designee shall ensure that students and staff who use the school Internet facilities receive appropriate training including the following:

- A. The district established standards for the acceptable use of the Internet;
- B. Internet safety rules;
- C. Rules for limited supervised access to and appropriate behavioral expectations for use of online resources, social network websites, and chat rooms;
- D. Cyberbullying (Board Policy 5131.1 Harassment, Intimidation and Bullying) awareness and response.

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

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.

ACCEPTABLE USE OF THE INTERNET

Purpose

To support its commitment to providing avenues of access to the universe of information available, the district's system of electronic communication shall include access to the Internet for students and staff.

Limitation of Liability

The Internet constitutes an unregulated collection of resources that changes constantly, so it is not possible to totally predict or control the resources that users may locate. The Board cannot guarantee the accuracy of the information or the appropriateness of materials that a user may encounter. Furthermore, the Board shall not be responsible for any damage users may suffer, including but not limited to, loss of data or interruptions of service. Nor shall the Board be responsible for financial obligations arising through the unauthorized use of the system.

District Rights and Responsibilities

The computer system is the property of the district, and all computer software and hardware belong to it. Therefore, the district retains the right to monitor all access to and use of the Internet.

The Board designates the Superintendent as the coordinator of the district system. He/she shall recommend to the Board of Education qualified staff persons to ensure provision of individual and class accounts necessary for access to the Internet, designation of quotas for disk usage on the system, establishment of a document retention schedule, establishment of a virus protection process and coordination of other activities as required to maintain the system.

Each Principal shall coordinate the district system in his/her building by approving all activities for that building; ensuring that teachers receive proper training in the use of the system; ensuring that students are adequately supervised when using the system; maintaining executed user agreements; and interpreting this acceptable use policy at the building level.

Access to the System

This Acceptable Use Policy shall govern all use of the system. Sanctions for student misuse of the system shall be included in the disciplinary code for students, as set out in regulations for Policy 5131 Conduct/Discipline. Employee misuse may result in appropriate discipline in accord with the collective bargaining agreement and applicable laws and regulations.

The Board shall ensure the acquisition and installation of blocking/filtering software to deny access to certain areas of the Internet.

World Wide Web

All students and employees of the Board shall have access to the Web through the district's networked or stand alone computers. An agreement shall be required. To deny a child access, parents/ guardians must notify the building Principal in writing.

Individual E-mail Accounts for Students

Students in grades K-8 may have individual accounts at the request of teachers and with the consent of parents/guardians. An individual account for any such student shall require an agreement signed by the student and his/her parent/guardian.

Individual E-mail Accounts for District Employees

District employees shall be provided with email access. Access to the system will be provided for staff members who have signed the acceptable use policy agreement. Email will be monitored and archived for three years. Employee email is discoverable and will be released if subpoenaed within the archival period set forth in this policy.

District Web Site

The Board authorizes the Superintendent to establish and maintain a district web site. The purpose of the web site will be to inform the district educational community of district programs, policies and practices.

Individual schools and classes may also establish web sites that include information on the activities of that school or class. The building Principal shall oversee these web sites along with the Supervisor of Technology.

The Supervisor of Technology shall publish and disseminate guidelines on acceptable material for these web sites. The Superintendent and Supervisor of Technology 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 Superintendent shall ensure that parents/guardians are notified about the district network and the rules governing its use. Parents/guardians shall sign an agreement to allow their child(ren) to have an individual account. Parents/guardians who do not wish their child(ren) to have access to the Internet must notify the Principal in writing.

Acceptable Use

Student Safety Practices

Students shall not post personal contact information about themselves or others. Nor shall students engage in any kind of personal contact with individuals they meet online. Attempts at contact from such individuals shall be reported immediately to the staff person monitoring that child's access to the Internet. Personal contact information includes but is not limited to names, home, school and work addresses, telephone numbers, or personal photographs.

Prohibited Activities

Users shall not attempt to gain unauthorized access (hacking) to the district system or to any other computer system through the district system, nor shall they go beyond their authorized access. This includes attempting to log in through another individual's account or accessing another's files.

Users shall not deliberately attempt to disrupt the district's computer system performance or destroy data by spreading computer viruses, worms, "Trojan Horses," trap door program codes or any similar product that can damage computer systems, firewalls, servers or network systems.

Users shall not use the district system to engage in illegal activities.

Users shall not access material that is profane or obscene, that advocates illegal acts, or that advocates violence or hate. Inadvertent access to such material should be reported immediately to the supervising staff person.

Users shall not plagiarize material that is available on the Internet. Plagiarism is presenting another's ideas/words as one's own.

Users shall not infringe on copyrighted material and shall follow all dictates of copyright law and the applicable policies of this district.

Prohibited Language

Prohibited language applies to public messages, private messages, and material posted on web pages.

Users shall not send or receive messages that contain obscene, profane, lewd, vulgar, rude, inflammatory, or threatening language.

Users shall not use the system to spread messages that can reasonably be interpreted as harassing, discriminatory or defamatory.

System Security

Users are responsible for their accounts and should take all reasonable precautions to prevent unauthorized access to them. In no case should a user provide his/her password to another individual.

Users shall immediately notify the supervising staff person or Technology Department if they detect a possible security problem. Users shall not access the system solely for the purpose of searching for security problems.

Users shall not install or download software or other applications without permission of the supervising staff person or Supervisor of Technology.

Users shall follow all district procedures when installing or downloading approved software.

System Limits

Users shall access the system only for educational, professional or career development activities. This applies to discussion group mail lists, instant message services and participation in Internet "chat room" conversations.

Users shall check e-mail frequently and delete messages promptly.

Privacy Rights

Users shall respect the privacy of messages that they receive and refrain from reposting messages without the approval of the sender.

Users shall not publish private information about another individual.

School Furnished Electronic Devices

The district may furnish students electronic devices such as laptop computers, tablets, notebooks, cellular telephones, or other electronic devices. When a student is furnished with an electronic device the district 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 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 or guardian of the student furnished an electronic device shall acknowledge receipt of the notification. The district shall retain the acknowledgement as long as the student retains the use of the electronic device.

Failure to provide the required notification shall be subject to a fine of \$250 per student, per incident.

Implementation

The Superintendent may prepare regulations to implement this policy, if necessary.

Adopted: July 26, 2010, February 24, 2014
NJSBA Review/Update: December 2015
Readopted: 8/22/16

Key Words

Acceptable Use, Blocking/Filtering Software, E-mail, Internet, Internet Safety, Technology, Web Site, World Wide Web, CIPA

Legal References:

<u>N.J.S.A.</u> 2C:20-25	<u>N.J.S.A.</u> 2A:38A-1 <u>et seq.</u> Computer System Computer Related Theft
<u>N.J.S.A.</u> 18A:7A-10	NJQSAC
<u>N.J.S.A.</u> 18A:36-35	School Internet websites; disclosure of certain student information prohibited
<u>N.J.S.A.</u> 18A:36-39	Notification by school to certain persons using certain electronic devices; fine
<u>N.J.A.C.</u> 6A:30-1.1 <u>et seq.</u>	Evaluation of the Performance of School Districts

17 U.S.C. 101 - United States Copyright Law

47 CFR 54.503(d) - Competitive Bidding: Gift Restrictions

47 U.S.C. 254(h) - Children's Internet Protection Act

Jersey v. T.L.O., State in re T.L.O., 94 N.J. 331 (1983), reversed on other grounds, New
569 U.S. 325 (1985).

O'Connor v. Ortega 480 U.S. 709 (1987)

No Child Left Behind Act of 2001, Pub. L. 107-110, 20 U.S.C.A. 6301 et seq.

Possible

<u>Cross References:</u>	*1111	District publications
	*3514	Equipment
	3543	Office services
	*3570	District records and reports
	4118.2/4218.2	Freedom of speech (staff)
	*5114	Suspension and expulsion
	*5124	Reporting to parents/guardians
	*5131	Conduct/discipline
	*5131.1	Harassment, intimidation and bullying
	*5131.5	Vandalism/violence
	*5142	Student safety
	5145.2	Freedom of speech/expression (students)
	*6144	Controversial issues
	*6145.3	Publications
	6161	Equipment, books and materials

*Indicates policy is included in the Critical Policy Reference Manual.

Exhibit

ACCEPTABLE USE OF TECHNOLOGY

The district's technology resources facilitate educational advancement. The following code of conduct will be adhered to for continued system use at Clinton Township School District and is applicable to all users, including students, faculty, support staff, and guest users.

DO:

1. Read and understand Clinton Township Board of Education's Policy 6142.10 Internet Safety and Technology, which includes Acceptable Use of the Internet (<http://www.ctsd.k12.nj.us/Board-of-education/policy/>).
2. Take care of equipment entrusted to you. It is the property of the district (and by extension the community). Treat it better than your own.
3. Become familiar with your school's technology assets. We want you to be knowledgeable in their use.
4. Ask questions when unsure. You can email the Technology Department at tech@ctsd.k12.nj.us.
5. Understand that you are responsible for your account and all activity within your account.

DO NOT:

1. Use the network to facilitate illegal activity.
2. Use the network for commercial or for profit purposes.
3. Use the network for non-school related work on more than an incidental basis.
4. Use the network for product advertisement or political lobbying.
5. Use the network for hate mail, discriminatory remarks, and offensive or inflammatory communication.
6. Illegally install, distribute, reproduce, or misuse copyrighted materials.
7. Use the network to access obscene or pornographic material.
8. Use inappropriate language or profanity on the network.
9. Use the network to transmit material likely to be offensive or objectionable to recipients.
10. Use the network to intentionally obtain or modify files, passwords, and data belonging to other users.
11. Use network facilities for fraudulent copying, communications, or modification of materials in violation of copyright laws.
12. Use the network to disrupt the work of other users.
13. Impersonate another user.
14. Share your district password with, or allow a password to be used by, anyone else.
15. Load or use unauthorized games, programs, files, or other electronic media.

16. Destroy, modify, or abuse network hardware and software.
17. Quote personal communications in a public forum without the original author's prior consent.
18. Participate on unauthorized social networks.
19. Neglect or mistreat district equipment, including leaving computers in hot cars, near liquids, or in precarious positions.

Violations will result in appropriate disciplinary action. Criminal activity will be referred to the appropriate authorities.

Any questions, please contact the Technology Department at tech@ctsd.k12.nj.us.

Policy

SCHOOL FURNISHED ELECTRONIC DEVICE: DISTRIBUTION AND USE

The Clinton Township Board of Education is committed to providing the students of this district with the technology, tools and resources that enhance achievement for 21st century learners. Excellence in education requires that technology be seamlessly integrated throughout the educational program by staff and students. Increasing access to technology is essential for the future, and one of the learning tools of these 21st century students is the school furnished electronic device computer. The use of school furnished electronic devices by staff and students shall help empower students to maximize their full achievement potential and prepare them for transition to high school, college and the workplace.

Providing school furnished electronic devices will further effective teaching and learning by integrating technology into the curriculum during classes and outside of school and by providing access to educational resources via the Internet. Use of the Internet shall facilitate the continuous dynamic interaction among students, educators, parents and the extended community.

School Furnished Electronic Device Distribution

The Superintendent or his or her designee shall develop guidelines for the equable distribution of the available equipment by class or grade. The distribution of school furnished electronic devices shall not be discriminatory and in compliance with law and Board policies for non-discrimination (2224 and 6121).

Any staff member or student issued a school furnished electronic device shall be liable for any damage suffered during the period of its use. He/she shall be responsible for its safe return (Board Policy 3514 Equipment).

Student Use of School Furnished Electronic Devices

Students issued school furnished electronic devices shall bring them to school as required by the class or classes for which the device has been assigned. Students shall not be allowed to take the school furnished electronic device home at the end of the school day or week. Student use of school furnished electronic devices during school shall be according to school Policy 6142.10 Internet Safety and Technology. Teachers may set additional requirements for use in their classroom. Students who misuse, mistreat or intentionally damage/vandalize a school furnished electronic device shall be liable for the repair and/or replacement of the device or its

accessories and shall be subjected to discipline up to and including suspension in accordance with the school Code of Student Conduct (5131 Conduct and Discipline).

Students misusing the Internet, accessing unauthorized Internet locations or participating in any activities in violation of Board Policy 6142.10 Internet Safety and Technology shall be subjected to discipline up to, and including suspension and expulsion in accordance with the school Code of Student Conduct (5131).

School Furnished Electronic Devices

The district may furnish students with electronic devices such as laptop computers, tablets, notebooks, cellular telephones, or other electronic devices. When a student is furnished with an electronic device the district 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 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 or guardian of the student furnished an electronic device shall acknowledge receipt of the notification. The district shall retain the acknowledgement as long as the student retains the use of the electronic device.

Failure to provide the required notification shall be subject to a fine of \$250 per student, per incident.

Staff members issued school-owned electronic devices shall have no expectation of privacy in the use of such device. The technology device may have security settings, monitoring or auditing software, tracking technology, and any other software that could monitor the use of the technology device;

Adopted: February 24, 2014
NJSBA Review/Update: December 2015
Readopted: 11/21/16

Key Words

school furnished electronic device, Internet, Equipment, Technology

Legal References:

N.J.S.A. 2C:20-25
N.J.S.A. 18A:7A-10
N.J.S.A. 18A:11-1

N.J.S.A. 2A:38A-1 et seq. Computer System
Computer Related Theft
NJQSAC
General mandatory powers and

duties

schools)

N.J.S.A. 18A:36-35 School Internet websites; disclosure of certain student information prohibited

N.J.S.A. 18A:36-39 Notification by school to certain persons using certain electronic devices; fine

N.J.S.A. 18A:54-20 Powers of Board (county vocational)

N.J.A.C. 6A:19-6.7 Securing machines and equipment

17 U.S.C. 101 - United States Copyright Law

47 CFR 54.503(d) - Competitive Bidding; Gift Restrictions

47 U.S.C. 254(h) - Children's Internet Protection Act

Jersey v. T.L.O., 94 N.J. 331 (1983), reversed on other grounds, New Jersey v. T.L.O., 469 U.S. 325 (1985).

No Child Left Behind Act of 2001, Pub. L. 107-110, 20 U.S.C.A. 6301 et seq.

Possible

Cross References:

*1330	Use of school facilities
*2224	Nondiscrimination/affirmative action
*3250	Income from fees, fines, charges
*3514	Equipment
*3516	Safety
*5114	Suspension and expulsion
*5124	Reporting to parents/guardians
*5131	Conduct/discipline
*5131.1	Harassment, intimidation and bullying
*5131.5	Vandalism/violence
*5142	Pupil safety
*6121	Nondiscrimination/affirmative action
*6142.10	Internet safety and technology
*6144	Controversial issues
6161	Equipment, books and materials

*Indicates Policy is included in the Critical Policy Reference Manual.

Regulation

SCHOOL FURNISHED ELECTRONIC DEVICE: DISTRIBUTION AND USE

To receive a school furnished electronic device, the staff member or parent/guardian and student must sign a school furnished electronic device agreement form that includes but may not be limited to the following provisions:

- A. School furnished electronic devices shall be used for the sole and express purpose of conducting school work or official school business;
- B. The use of all school furnished electronic devices is subject to the district's Acceptable Use of Technology Policies (4119.26/4219.26 Electronic Communication between Staff and Students and 6142.10 Internet Safety and Technology) and any other Board policies regarding appropriate and acceptable conduct;
- C. All school furnished electronic devices are considered the property of the Board and shall be returned:
 1. By students at the end of the school semester or school year as assigned;
 2. By staff upon termination of employment with the district or immediately upon request by the Superintendent;
- D. School furnished electronic devices may include the district's software image and preloaded software for specific tasks. The installation of other software images or software on school furnished electronic devices shall be approved and may only be done by the assigned staff member authorized to maintain the equipment;
 1. Students and school furnished electronic devices to any other person unless authorized to do so by the Superintendent or his or her designee;
 2. Store the electronic device when not in use only in a securely locked area. Do not leave the technology device unattended at any time in an unsecured location; and
 3. Keep the school furnished electronic device in sight at all times while in public places;
- E. The staff member or the parent/guardian shall be responsible to reimburse the school district the cost of any school furnished electronic device that is lost, damaged beyond reasonable use or beyond its value, abandoned, missing, stolen, or cannot be returned to the district;
- F. Students and staff members may be required to provide routine cleaning and care of the electronic device as needed;

- G. When a staff member or student has reason to believe the technology device may have been stolen, the following procedure shall apply:
 - 1. Immediately report the incident to the issuer of the device;
 - 2. File an official police report documenting the theft; and
 - 3. Provide a copy of the police report to the school;
- H. A student or staff member shall report any hardware or software problems in the operation of the device to assigned staff member authorized to maintain the equipment;
- I. The Board is under no legal, financial, or other obligation to provide a replacement electronic device to any individual whose device is lost, stolen, or damaged;
- J. All school furnished electronic devices are the property of the Board. The individual issued the electronic device shall have no expectation of privacy in the use of such device. The technology device may have security settings, monitoring or auditing software, tracking technology, and any other software that could monitor the use of the technology device;
- K. Any student who is issued a school furnished electronic device shall be notified in writing or through 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;
- L. Students are responsible for having the electronic device fully charged for the class or classes in which the device will be used. Failure to have the device in class or not charged for class may result in disciplinary action for being unprepared for class;
- M. The assigned staff member authorized to administer and implement the issuance of school furnished electronic devices to staff members shall:
 - 1. Maintain direct oversight of the inventory of devices, service contracts, agreements, and internal controls for all school district provided technology devices provided to staff members; and
 - 2. Ensure compliance with regulatory policies and procedures as applicable.

Any violation of Board policies or procedures including, but not limited to, school district provided technology devices to staff members; acceptable use of computer networks, computers, and resources; and/or inappropriate conduct may result in appropriate disciplinary action. Disciplinary action may include the revocation of the agreement and the immediate return of the device to the school. A copy of Board Policy and Regulation 3514.1 School Furnished Electronic Devices shall be attached to the agreement. The agreement shall be signed by any staff member or student and his or her parent/guardian who receives a school furnished electronic device.

Adopted: February 24, 2014

NJSBA Review/Update: December 2015

Readopted: 11/21/16

N. staff members that are furnished school-owned electronic devices are expected to take all appropriate measures and precautions to prevent the loss, theft, damage, and/or unauthorized use of such technology devices. These appropriate measures and precautions shall include, but are not limited to, the following:

4. Keep the school furnished electronic device in a locked and secured environment when not being used;
5. Do not leave the electronic device in a vehicle for prolonged periods of time, especially in extreme temperatures;
6. Keep food and drinks away from all electronic devices and work areas;
7. Do not lend the